UNCLASSIFIED CONTROLLED INFORMATION

A. GENERAL.

1. Unclassified Controlled Information (UCI) [formally known as Sensitive Unclassified Information (SUI)] is any information, regardless of its physical form or characteristics, which has been determined to have relative sensitivity and requires mandatory protection because of statutory or regulatory restrictions or which requires a degree of discretionary protection due to the risk to national or United States (U.S.) Department of Energy (DOE) interests or to the magnitude of loss or harm that could result from the inadvertent or deliberate misuse, alteration, disclosure, or destruction of such information.

2. The DOE Savannah River Site UCI categories utilized and controlled by bidders include:

   - Unclassified Controlled Nuclear Information (UCNI)
   - Official Use Only (OUO)
   - Export Controlled Information (ECI)

3. The term “need-to-know" is defined as a determination by a person having responsibility for UCI that a proposed recipient's access to such information is necessary in the performance of official or contractual duties of employment. The need-to-know principle is essential to the protection of UCI.

4. The purpose of this document is to assist bidders in the identification of UCI and to provide protective measures for UCI from its receipt or origination until its destruction. Protective measures for UCI will minimize the probability of inadvertent disclosure of UCI by bidders while increasing the difficulty of illegally obtaining UCI. None of these protective measures are intended to deny the general public of the United States access to any information to which they have a legal right to know.

B. UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION.

1. Categories. If you produce a document that contains any of the following categories, the document must be reviewed for UCNI by an authorized RO:

   - Designs of nuclear production or utilization facilities
   - Safeguards and security information regarding nuclear facilities or material
   - Declassified nuclear weapon information that at a later date is considered to be sensitive

   The following items are an example of UCNI in a SRS Sensitive Facilities (i.e., Tritium facility):

- Layouts/floor plans
- Special Nuclear Material storage locations
- Structural design details
- Dispersal of radioactive material
- Fixed process equipment details/location
- Piping, instrumentation, logic or writing diagrams
- Glovebox layouts

NOTE: If the document/data is not clearly concerned with these categories, it is not UCNI.

2. Responsibilities for Review of Matter. Anyone who thinks unclassified matter they create or come into possession of may contain UCNI, must send that matter to a RO before the matter is finalized, sent outside of the organization, or filed. The only exception is matter that is to be destroyed right away. More detailed information can be found in DOE M 471.1-1, Chapter I, Part B, Review of Matter.

3. Marking. Specific detailed requirements for the marking of UCNI can be found in DOE M 471.1-1, Chapter I, Part C, Marking of Matter. Specific examples of markings for media, indicating their use, format, and placement, are included in Appendix E of this manual. The DOE Classified Matter Protection and Control Marking Handbook, Version 2.0, March 2003, contains an example of marking an UCNI document, but not for classified media. This handbook is on the internet at http://www.ntc.doe.gov/Courses/Online.

   a. Documents marked UCNI contain UCI that is not subject to disclosure under the Freedom of Information Act (FOIA).

   b. The preliminary review determination and the marking "May Contain UCNI" is no longer used.

   c. Removable computer media containing UCNI must be labeled with the Standard Form (SF) 710, "Unclassified" label and marked "UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION" or "UCNI" on the classification line of the SF 711, Data Descriptor. Also, an OSR Form 10-292, label, "Unclassified Sensitive Information," must be affixed to any removable media containing UCNI. Refer to Appendix E of this manual.

   d. The sender must notify the recipient of the level of UCI within the subject line of the email (UCNI, OUO, or ECI). The first line of an e-mail message containing UCNI information must include the abbreviation "UCNI" before the beginning of the text. If the message itself is not

UCNI but an attachment is, the message must indicate that the attachment is UCNI.

4. Access. Provided only to those authorized routine or special access.

   a. Routine Access. Routine access refers to the normal exchange of UCNI during the conduct of official business and allows for further dissemination of UCNI if certain requirements are met (See DOE M 471.1-1, "Identification and Protection of UCNI," Chapter II, Paragraph 1.a.2).

   b. Non-U.S. Citizen Not Eligible for Routine Access. Submit request to SR, Director, OSSES within 60 days prior to requiring access to UCNI. Refer to DOE M 471.1-1, "Identification and Protection of UCNI, Chapter II Paragraph 1.a.(2)(c) for additional information.

   c. Special Access. An individual not authorized routine access may be approved for special access (i.e., attorney representing an employee in litigation with DOE). Submit request to SR, Director, OSSES within 60 days prior to requiring access to UCNI. Detailed direction for the requesting and approving of requests for special access can be found in DOE M 471.1-1, "Identification and Protection of Unclassified Controlled Nuclear Information," Chapter II, Paragraph 1.b.

5. Physical Protection.

   a. In Use. Any individual authorized access to UCI must maintain physical control over the matter to prevent unauthorized access to the information.

   b. In Storage.

      UCI must be secured behind a locked door or in a locked container/desk when unattended; or in a method which would prevent/preclude unauthorized disclosure.

   c. Information Systems.

      - Password protected or on removable media
      - With distribution restricted to those with established need-to-know
      - Be clearly marked as appropriate

   d. Transmission.

      (1) Mail Transmission. UCI must be in a single sealed opaque envelope or wrapping and addressed to the recipient to include

marking "TO BE OPENED BY ADDRESSEE ONLY." Packages may be sent as follows:

- Hand-carried
- U. S. Mail by First Class, Express, Certified, or Registered Mail
- Any commercial carrier (e.g., Federal Express, Emery, etc.) using signature service

(2) Over Telecommunication Circuits:

UCI must be protected by approved encryption when transmitted off site by telecommunications services. UCI transmitted over public-switched broadcast communications paths (e.g., Internet) then the information must be protected by approved encryption.

e. Reproduction. Matter marked as containing UCI may be reproduced without the permission of the originator to the minimum extent necessary consistent with need to carry out official duties and need-to-know as long the matter is not marked as "Dissemination Controlled." Any copy machine malfunctions must be cleared to ensure no UCI matter is left in the machine.

f. Destruction.

(1) The normal method for destroying documents containing UCI is by using a strip-cut shredder that outputs strips not exceeding ¼-inch wide. This may be done in workplace, if a strip shredder is available.

(2) Computer storage media such as floppy disks, ZIP, JAZ cartridges, hard drives, CDs, etc., containing UCI must be destroyed by shredding/chipping, crushing or burning or returned to the SR Office of Contracts Management .

Prior to sending bidder equipment or media containing SR information to an offsite vendor for repair or warranty credit or redeployment, the SR information must be cleared by the bidder.

6. Loss or Unauthorized Disclosure. Any person who determines that UCI has been or may have been lost or disclosed without authority must immediately report this information to the SR Security Incident Program Manager (803-725-8936) as a security incident. A determination must be made as to whether an infraction or a violation has occurred. Unauthorized disclosure of any UCI that is protected by the Privacy Act, other Federal statutes, or site policy and procedure may result in civil or criminal sanctions or administrative action against responsible persons.

The SR Office of Contracts Management that provided the UCI will be informed of its unauthorized disclosure.

C. OFFICIAL USE ONLY.

1. Guidelines.

   a. DOE guidance for OUO determination (statutory text, detailed discussion, and examples of each exemption) is based on DOE Guide (G) 471.3-1.

   b. All information designated by SR as OUO, if subject to a FOIA request, will be managed in accordance with DOE G 1700.1. Based on the FOIA request and a determination by an SR Authorizing Official, who conducts an independent evaluation, the SR designated OUO may be released in part or whole or release may be denied, based on reasonably foreseeable harm and the public interest.

2. Categories of OUO. Seven of the nine categories of information exempt from the publication and disclosure requirements of the FOIA, as detailed in DOE G 471.3-1, "Guide to Identifying Official Use Only Information," are designated as OUO by SR. These seven categories of OUO information are listed below by Exemption Number corresponding to the original FOIA Exemption Number. The FOIA exemptions provide the basis for non-disclosure and generally are discretionary rather than mandatory.

   Exemption 1 is not listed here because that exemption applies only to information that has been formally classified by an Executive Order. This information could never be OUO.

   Exemption 3 is not listed here because that exemption applies to information explicitly prohibited from disclosure by a statute passed by Congress. Within DOE, this exemption applies to the Atomic Energy Act, which is the basis for control of Restricted Data, Formerly Restricted Data, and UCNI. This information could never be OUO.

   a. Exemption Two - Circumvention of Statute. This exemption concerns information related solely to the internal personnel rules and practices of SR.

   b. Exemption Four - Commercial/proprietary. This exemption concerns trade secrets and commercial or financial information of a privileged or confidential nature obtained from a person.

   c. Exemption Five - Privileged Information. This exemption concerns inter-agency or intra-agency memoranda or letters which would not be available by law to a party other than an agency in litigation with the agency.

d. Exemption Six - Personal Privacy. This exemption concerns personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

e. Exemption Seven - Law Enforcement. This exemption concerns records or information compiled for law enforcement purposes, but only to the extent stipulated in DOE G 471.3-1.

f. Exemption Eight - Financial Institutions. This exemption concerns information contained in or related to examination, operating, or condition reports prepared by, or on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions.

g. Exemption Nine - Wells. This exemption concerns geological and geophysical information and data, including maps, concerning wells.

3. Identification of OUO. In order to qualify as OUO, information must be unclassified; be included within one of the exemptions listed in Paragraph C.2. above; be created or obtained by SR; and be under SR control. Any employee who has cognizance over such information may determine whether the document contains OUO information. The document originator is responsible to identify and mark documents containing OUO information if deemed necessary for the protection of the information.

4. Access. OUO access may be granted to bidder and bidder employees with an established need-to-know for the OUO in the performance of official or contractual duties. The responsibility to determine need-to-know rests with the person who has authorized possession, knowledge, or control of the information. If the OUO involves information subject to the Export Administration Regulation, the SR Export Control Program Manager shall be contacted prior to the release of the OUO information to a foreign national employee.

5. Marking Requirements.

a. If the originator determines a document should be protected as OUO, the first page of the document must be marked with the following or similar statement:

OFFICIAL USE ONLY
May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number and category: _____
Department of Energy review required before public release
Name/Org: _____Date:_____
Guidance (if applicable)_____

b. The marking "**OFFICIAL USE ONLY**" (or **OUO** if space is limited) must be placed on the bottom of each subsequent page of the document or just the pages containing OUO information.

c. The marking of removable media and e-mail messages for OUO is the same as stated for UCNI in Paragraph B.6.d. and B.6.e. above.

d. Refer to DOE M 471.3-1, Chapter I, Paragraph 3, "Manual for Identifying and Protecting Official Use Only Information" for additional information on markings.

6. Physical Protection. All physical protection requirements for OUO are the same as stated for UCNI in Paragraph B.5. above (in use, in storage, information systems, reproduction, and destruction).

7. Unauthorized Disclosure. Unauthorized disclosure of any OUO that is protected by the Privacy Act, other Federal statutes, or site policy and procedure may result in civil or criminal sanctions or administrative action against responsible persons. The SR Office of Contracts Management that provided the OUO will be informed of any unauthorized disclosure.

D. EXPORT CONTROLLED INFORMATION.

1. Export Controlled Information. ECI is any technical information determined to contain technical data, the export of which is restricted by:

- 10 CFR 810, DOE Assistance to Foreign Atomic Energy Activities, or
- 15 CFR 774, U.S. Department of Commerce (DOC) Export Administration Regulations, Commerce Control List, Supplement 1, or
- 22 CFR 121, U.S. Department of State (DOS) U.S. Munitions List, or
- DOE export control guidance.

If exported, ECI requires a technology export license or authorization under United States export regulations. Typical nuclear-related ECI encountered at the SRS would include nuclear fuel cycle, heavy water, and tritium production technology.

2. Non-Public Technical Data (NPTD). NPTD is technical data which is not publicly available and which is not specifically identified in 10 CFR 810, 15 CFR 774 - Supplement 1, or 22 CFR 121. The U.S. DOC requires an export license review prior to transferring NPTD to a foreign national (deemed export) or transferring NPTD out of the U.S.

3. Deemed Export. A domestic release of export controlled technology or source code to a foreign national who is not a person lawfully admitted for permanent residence in the United States (e.g., holder of a green card) or a protected individual (e.g., refugee) under the Immigration and Naturalization Act [8 USC 1324B (a) (3)].

4. Export. An actual shipment, transmission, or release of items, technology, or software out of the United States.

5. Release. Release occurs when NPTD or ECI leaves the bidder's control or is transferred to a foreign national.

6. Release of Technology or Source Code. Technology or source code is "released" for export through:

   a. Visual inspection by foreign nationals of U.S. - origin equipment and facilities;

   b. Oral exchanges of information in the United States or abroad; or

   c. The application to situations abroad of personal knowledge or technical experience acquired in the United States.

7. Technology. Specific information necessary for the development, production, or use of a product. The information takes the form of technical data or technical assistance.

   NOTE 1: Technical assistance -- May take forms such as instruction skills training, working knowledge, or consulting services.

   NOTE 2: Technical assistance may involve transfer of technical data.

8. Technical Data. May take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, and read-only memories.

9. Access. ECI access may be granted to bidder employees who are U.S. Citizens with established need-to-know in the performance of official or contractual duties. Foreign nationals may be given access to NPTD if approved by the SR Export Control Program Manager (ECPM) only after a need-to-know is established for the foreign national and an export license or authorization has been obtained from the appropriate U.S. agency (i.e., DOC, DOS, or DOE), if required. Export licenses or authorizations are for a specific technology and do not authorize access to any other technology without another specific EC review. The approval of the SR ECPM should be obtained prior to the release of ECI or NPTD to any foreign national no matter what form the technical data may take.

10. Originator. The originator of a document is responsible for the initial identification and protection of NPTD and ECI and must seek out an Export Control Reviewer to conduct a formal review if the information is being considered for release outside the DOE or to any foreign national. (Contact the SR Office of Contracts Management)

11. EC Reviewer. An individual, who by familiarization and/or experience is considered a subject matter expert, authorized to make a determination that equipment, material, or technical information is or is not export controlled. (Contact the SR Office of Contracts Management)

12. Marking Requirements. Products containing ECI must be clearly marked in accordance with the following procedures:

a. The following statement must be marked on the cover or first page of any information product determined to contain ECI:

"EXPORT CONTROLLED INFORMATION"

Contains technical data whose export is restricted by statute. Violations may result in administrative, civil, or criminal penalties. Limit dissemination to U.S. citizens who are U.S. Department of Energy (DOE) employees or DOE contractors or employees of other U.S. Government agencies. The cognizant program manager must approve other dissemination. This notice shall not be separated from the attached document.

_____

Reviewer (Signature)

_____

Date

_____

Source Document

b. The bottom of each interior page determined to include ECI must be marked:

"EXPORT CONTROLLED INFORMATION"

c. The marking of removable media and e-mail messages for ECI is the same as stated for UCNI in Paragraph B.5.

d. Documents, faxes, e-mails, containing technical data being released to U.S. Government agencies and their contractors (U.S. citizens only) do not require an export control review if marked:

CONTAINS NON-PUBLIC TECHNICAL DATA
Requires Export Control Review Prior to Release to the Public or any Foreign National.

13. Physical Protection. All requirements for ECI are the same as stated for UCNI in B.5. above (in use, in storage, information systems, reproduction, and destruction).

14. Unauthorized Disclosure. Direction for unauthorized disclosure is the same as stated for UCNI information in Paragraph B.6. above. Unauthorized disclosure of ECI can also result in administrative, civil, or criminal penalties including fines and imprisonment.